Configure and verify IPv4 addressing and subnetting

Configure and verify IPv6 addressing and prefix

- **1 Configure and verify VLANs (normal range) spanning multiple switches**
  - **2.1.a Access ports (data and voice)**
  - **2.1.b Default VLAN**
  - **2.1.c InterVLAN connectivity**

- **2.2 Configure and verify interswitch connectivity**
  - **2.2.a Trunk ports**
  - **2.2.b 802.1Q**
  - **2.2.c Native VLAN**

- **2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)**

- **2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)**

- **3.3 Configure and verify IPv4 and IPv6 static routing**
  - **3.3.a Default route**
  - **3.3.b Network route**
  - **3.3.c Host route**
  - **3.3.d Floating static**

- **3.4 Configure and verify single area OSPFv2**
  - **3.4.a Neighbor adjacencies**

- **3.4.b Point-to-point**
- **3.4.c Broadcast (DR/BDR selection)**
- **3.4.d Router ID**

- **4.1 Configure and verify inside source NAT using static and pools**

- **4.2 Configure and verify NTP operating in a client and server mode**

- **4.6 Configure and verify DHCP client and relay**

- **4.8 Configure network devices for remote access using SSH**

- **5.3 Configure and verify device access control using local passwords**

- **5.6 Configure and verify access control lists**

- **5.7 Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)**
- **5.10 Configure and verify WLAN within the GUI using WPA2 PSK**

Let's Continue Building Your Network

2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)

Cisco Discovery Protocol (CDP):

- Enables Cisco devices to automatically discover each other.
- Provides information about device type, platform, software version, IP address, and interface details.

Configuration:

enable

configure terminal

interface FastEthernet0/1

cdp enable

end

Verification:

show cdp neighbors

LLDP:

- Industry standard protocol for device discovery.
- Provides similar information to CDP, but with a wider vendor support.

Configuration:

enable

configure terminal

interface FastEthernet0/1

lldp enable

end

Verification:

show lldp neighbors

2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)

EtherChannel:

- Bundles multiple physical interfaces into a single logical interface.
- Increases bandwidth, redundancy, and load balancing.

Configuration:

```
interface Range FastEthernet0/1 - 2
 channel-group 1 mode active
end
```

Verification:

```
show etherchannel summary
show interface channel-group 1
```

3.3 Configure and verify IPv4 and IPv6 static routing

Static Routing:

- Manually configured routes between networks.

Configuration:

```
ip route 192.168.2.0 255.255.255.0 192.168.1.2
ipv6 route 2001:db8:2::/64 2001:db8:1::1
```

Verification:

```
show ip route
show ipv6 route
```

Default Route:

- A route to send traffic to an unknown destination.

Configuration:

```
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ipv6 route ::/0 2001:db8:1::1
```

Network, Host, and Floating Static Routes:

- Specific routes for specific networks, hosts, or redundancy.
- Configure as needed based on network design.

3.4 Configure and verify single area OSPFv2

OSPF:

- Interior gateway protocol for routing within an autonomous system.

Configuration:

router ospf 1

network 192.168.1.0 0.0.0.255 area 0

router-id 192.168.1.1

end

Verification:

show ip ospf neighbor

show ip ospf interface

show ip ospf process

Point-to-Point, Broadcast, and DR/BDR:

- OSPF operates differently in different network topologies.
- Point-to-point: Direct connection between two routers.
- Broadcast: Multiple routers connected to the same network segment.
- DR/BDR: Designated Router and Backup Designated Router for broadcast networks.

Router ID:

- Unique identifier for a router in OSPF.

4.1 Configure and verify inside source NAT using static and pools

NAT:

- Translates private IP addresses to public IP addresses.

Configuration:

ip nat inside source list STATIC interface FastEthernet0/0 overload

access-list 1 permit 192.168.1.10

ip nat inside source static 192.168.1.10 192.168.100.10

Verification:

show ip nat translations

4.2 Configure and verify NTP operating in a client and server mode

NTP:

- Synchronizes clocks across network devices.

Configuration:

ntp server 192.168.1.2

ntp authenticate

Verification:

show ntp status

Note: This is a basic outline and requires customization based on your specific network requirements. It's essential to follow best practices for network design, security, and troubleshooting.

Let's Configure and Verify Your Network

Understanding Your Environment

Before we dive into specific commands, it's essential to clarify:

- **Device type:** Are you working with Cisco routers, switches, or other devices?
- **Operating system:** Are you using a specific OS (e.g., Windows Server, Linux)?
- **Network topology:** How are your devices connected (star, ring, etc.)?
- **Desired functionality:** Do you want a DHCP server on a router, or a DHCP relay on a switch?

Assuming a Cisco Router Environment

4.6 Configure and verify DHCP client and relay

DHCP Server Configuration:

router(config)#ip dhcp pool POOL1

router(config-dhcp)#network 192.168.1.0 255.255.255.0

router(config-dhcp)#default-router 192.168.1.1

router(config-dhcp)#dns-server 8.8.8.8

router(config-dhcp)#exit

DHCP Relay Configuration:

interface FastEthernet0/1

ip helper-address 192.168.2.100 // Replace with DHCP server IP

Verification:

- Check DHCP pool configuration: show ip dhcp pool POOL1
- Check DHCP relay configuration: show ip interface FastEthernet0/1
- Verify DHCP client IP assignment: ipconfig /all on a client device

4.8 Configure network devices for remote access using SSH

Basic SSH Configuration:

enable

configure terminal

crypto key generate rsa

line vty 0 4

password <password>

transport input ssh

end

Verification:

- Test SSH connectivity using a SSH client.

5.3 Configure and verify device access control using local passwords

User Account Creation:

enable

configure terminal

username user1 password <password> privilege level 15

end

Verification:

- Attempt to login with the created user account.

5.6 Configure and verify access control lists (ACLs)

Standard ACL Example:

access-list 100 deny tcp any host 192.168.2.10

access-list 100 permit ip any any

Extended ACL Example:

access-list 101 deny tcp any any eq www <should be a port ## like 80

access-list 101 permit ip any any

Apply ACL:

interface FastEthernet0/0

ip access-group 100 in

Verification:

- Test network connectivity with and without ACLs.

5.7 Configure and verify Layer 2 security features

DHCP Snooping:

ip dhcp snooping

interface FastEthernet0/1

switchport mode access

switchport access vlan 10

ip dhcp snooping trust

Dynamic ARP Inspection:

ip arp inspection

interface FastEthernet0/1

ip arp inspection trust

Port Security:

interface FastEthernet0/1

switchport mode access

switchport port-security maximum 2

switchport port-security violation restrict

Verification:

- Test with rogue DHCP server, ARP spoofing, and exceeding maximum MAC addresses.

5.10 Configure and verify WLAN within the GUI using WPA2 PSK

Note: This configuration is typically done through a web-based interface on a wireless controller or access point. Specific steps will vary.

General Steps:

1. Access the device's web interface.
2. Navigate to the wireless configuration section.
3. Create a new SSID.
4. Select WPA2 PSK as the security mode.
5. Configure encryption settings (AES).
6. Set a strong pre-shared key (PSK).

Verification:

- Attempt to connect a wireless client using the configured SSID and PSK.

Remember: This is a basic outline. The specific commands and configuration options may vary depending on the device and operating system. Always refer to the device's documentation for accurate and detailed instructions.

Would you like to focus on a specific configuration or device?

Would you like to delve deeper into any specific area or provide more details about your network topology?